

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

-----	X	
	:	
UNITED STATES OF AMERICA,	:	
	:	No. 09-CR-1037 (RWS)
vs.	:	
	:	
PATRICK NAYYAR,	:	
	:	
Defendant.	:	
	:	
-----	X	

**MEMORANDUM OF LAW ON BEHALF OF DEFENDANT PATRICK NAYYAR
IN CONNECTION WITH PROCEEDINGS ON REMAND**

Laura Grossfield Birger
Stephanie B. Turner
COOLEY LLP
1114 Avenue of the Americas
New York, NY 10036
(212) 479-6000

*Attorneys for Defendant
Patrick Nayyar*

TABLE OF CONTENTS

	Page
PRELIMINARY STATEMENT	1
PROCEDURAL BACKGROUND.....	2
I. NAYYAR’S TRIAL AND MOTION FOR A MISTRIAL	2
II. NAYYAR’S APPEAL AND THE SECOND CIRCUIT’S SUMMARY ORDER	4
III. THE STIPULATION	5
ARGUMENT	6
THE EVIDENCE OBTAINED FROM MR. NAYYAR’S LAPTOP SHOULD HAVE BEEN SUPPRESSED.....	6
I. THE CONSENT OF NAYYAR’S WIFE WAS INVALID	6
A. Pertinent Facts.....	6
1. Nayyar’s Wife’s Consent to Search.....	6
2. The Initial Searches of the Laptop	7
B. Nosava Could Not Consent to the Search of Nayyar’s Laptop Because the Laptop Was Password-Protected and She Did Not Know the Password.....	8
C. The Initial Searches Were Unlawful In Light of Nosava’s Invalid Consent	12
II. THE INDEPENDENT SOURCE DOCTRINE DOES NOT APPLY	13
A. Pertinent Facts.....	13
B. The Independent Source Doctrine Does Not Apply Because the Government’s Search Warrant Application Was Prompted By the Prior, Unlawful Review	15
III. NAYYAR DID NOT WAIVE HIS RIGHT TO CHALLENGE THE LAPTOP EVIDENCE.....	17
A. The Timing of Discovery and Pretrial Motions to Suppress	17
B. Nayyar Had Good Cause For Not Challenging the Computer Search Prior to Trial.....	19
CONCLUSION.....	23

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	8
<i>Davis v. United States</i> , 411 U.S. 233 (1973).....	19
<i>Illinois v. Rodriguez</i> , 497 U.S. 177 (1990).....	11
<i>Murray v. United States</i> , 487 U.S. 533 (1988).....	15
<i>Trulock v. Freeh</i> , 275 F.3d 391 (4th Cir. 2001)	9, 10
<i>United States v. Buckner</i> , 473 F.3d 551 (4th Cir. 2007)	10
<i>United States v. Davis</i> , 967 F.2d 84 (2d Cir. 1992).....	9, 10
<i>United States v. Gonzalez</i> , 81 F. Supp. 3d 1212 (D.N.M. 2015)	22, 23
<i>United States v. Griswold</i> , 2011 U.S. Dist. LEXIS 153943 (W.D.N.Y. June 2, 2011)	10, 11
<i>United States v. Johnson</i> , 994 F.2d 980 (2d Cir. 1993).....	15, 16
<i>United States v. Jones</i> , 766 F.2d 994 (6th Cir. 1985)	19, 21
<i>United States v. McGee</i> , 564 F.3d 136 (2d Cir. 2009).....	9, 10
<i>United States v. Mutschelknaus</i> , 564 F. Supp. 2d 1072 (D.N.D. 2008).....	13
<i>United States v. Ortega</i> , 2007 U.S. Dist. LEXIS 82514 (M.D. Fla. Nov. 6, 2007)	16
<i>United States v. Sanchez</i> , 813 F. Supp. 241 (S.D.N.Y. 1993)	19, 20, 21, 22

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>United States v. Scott</i> , 607 F. App'x 191 (3d Cir. 2015)	19, 21
<i>United States v. Siciliano</i> , 578 F.3d 61 (1st Cir. 2009)	16
<i>United States v. Snype</i> , 441 F.3d 119 (2d Cir. 2006)	8
<i>United States v. Stabile</i> , 633 F.3d 219 (3d Cir. 2011)	10
<i>United States v. Syphers</i> , 426 F.3d 461 (1st Cir. 2005)	13
<i>United States v. Turner</i> , 23 F. Supp. 3d 290, 312-13 (S.D.N.Y. 2014)	11, 12
<i>United States v. Wilson</i> , 11 F.3d 346 (2d Cir. 1993)	19
Other Authorities	
Fed. R. Crim. P. 12	19

PRELIMINARY STATEMENT

Before this Court are three issues identified by the Court of Appeals for the Second Circuit regarding the search of Defendant Patrick Nayyar's laptop. Specifically, the Second Circuit directed this Court to consider whether (1) Nayyar waived his right to challenge the laptop evidence; (2) Nayyar's wife's consent was a valid legal basis for the search of the laptop; and (3) the independent source exception to the exclusionary rule applies.

These issues previously arose during Nayyar's trial before this Court, when Nayyar and his counsel learned for the first time that agents from the FBI searched his laptop without a valid legal basis and prior to obtaining a search warrant. As soon as Nayyar became aware of these facts during the testimony of a Government witness, he moved for a mistrial. This Court denied the mistrial motion, holding that Nayyar waived his challenge to the laptop evidence and, alternatively, that the laptop evidence inevitably would have been discovered and therefore qualified for an exception to the exclusionary rule. That ruling was based on incomplete facts proffered by the Government; no evidence or witnesses were presented. The jury found Nayyar guilty on all counts.

Nayyar appealed his conviction. The Court of Appeals held that the record was insufficient to support the denial of Nayyar's mistrial motion, and remanded to this Court for a post-trial hearing on the three issues identified above.

Following the Second Circuit's decision, the Government conducted further inquiry into the facts surrounding the laptop search, and the parties reached a stipulation regarding those facts. Now that the previously incomplete record has been supplemented, it establishes that Nayyar's wife did *not* give valid consent to the search of Nayyar's personal laptop; the record demonstrates that she lacked access to the laptop and did not have authority to consent. Accordingly, the pre-warrant searches of the laptop were unlawful. Moreover, the Government

cannot meet its burden under the independent source doctrine, and therefore, that exception to the warrant requirement does not justify the admission of the laptop evidence. Finally, Nayyar did not waive his challenge to his wife's consent because he raised it as soon as he became aware of the pre-warrant search. Under these circumstances, Nayyar had good cause for not raising the issue prior to trial.

PROCEDURAL BACKGROUND

I. NAYYAR'S TRIAL AND MOTION FOR A MISTRIAL

Nayyar's trial on the following five counts began on March 19, 2012:

- (Count 1) conspiracy to provide material support to Hizballah, a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B;
- (Count 2) provision of material support to a designated foreign terrorist organization in violation of 18 U.S.C. §§ 2339B & 2;
- (Count 3) conspiracy to provide funds, goods, or services to and for the benefit of Hizballah in violation of 50 U.S.C. § 1705(a) and 31 C.F.R. §§ 595.204, 595.205 & 595.311;
- (Count 4) provision of funds, goods, or services to and for the benefit of Hizballah in violation of 50 U.S.C. § 1705(a), 18 U.S.C. § 2 and 31 C.F.R. §§ 595.204, 595.205 & 595.311; and
- (Count 5) conspiracy to traffic in firearms and ammunition without a license in violation of 18 U.S.C. § 371.

On the first and second days of trial, Special Agent Candace Hunter ("Agent Hunter"), a forensic examiner in the Computer Analysis Response Team ("CART") of the Federal Bureau of Investigation ("FBI"), testified at length about what the FBI found on Nayyar's laptop, which the FBI seized at the time of his arrest. Through Agent Hunter's testimony, the Government introduced numerous exhibits showing that an individual using Nayyar's account visited websites relating to weapons and military equipment and an article relating to Hizballah.

On cross examination, Nayyar's counsel questioned Agent Hunter regarding the searches she had conducted on the laptop. (Tr. 104-05.)¹ Agent Hunter explained that she "commenced [her] search" of the laptop on December 2, 2009, although a search warrant was not obtained until October 29, 2010. (*Id.*) She also testified that Nayyar's laptop was protected by a password, and that she accessed the laptop in December 2009 without knowing the password. (Tr. 102-03.) Based on this testimony, Nayyar and his counsel learned for the first time that the FBI had searched Nayyar's laptop without a warrant or valid consent.

Following Agent Hunter's testimony, Nayyar moved for a mistrial because the Government had already introduced a significant amount of prejudicial evidence from the unlawful searches. (Tr. 190-91.) Defense counsel explained to the Court that:

Mr. Nayyar, in order to get a fair trial and to be represented properly in this case, should have had . . . a motion filed regarding the search of the computer, and that wasn't done. . . . As his attorney now, the trial attorney, at the first moment I understood that to be an issue, I'm bringing it to the Court's attention.

(Tr. 191.)² The Government responded that the FBI agents believed they had consent from Nayyar's wife, Maryna Nosava, to search the laptop in December 2009, and that the agents had obtained the password from Nayyar. (Tr. 193.) The Government argued further that even if the consent were invalid, the evidence inevitably would have been discovered and therefore qualified for an exception to the exclusionary rule. (Tr. 196-97.)

Initially, this Court asked the Government to recall Agent Hunter for a hearing. (Tr. 195.) However, when the Government called Hunter on the phone, she was already on her way out of the state. (Tr. 229.) The Government thus relayed to the Court what Hunter said during the phone conversation. According to the Government's proffer, Hunter received the laptop in

¹ Citations to the trial transcript are denominated "Tr. __." For the Court's convenience, all pages cited from the transcript are attached to this memorandum of law as Exhibit 1.

² Nayyar changed counsel several times prior to trial.

December 2009, “along with a consent to search form which purported to give consent for the computer.” (*Id.*) The Government related that Agent Hunter said she copied and processed the hard drive in 2009, but did not review it in detail. (*Id.*) After Hunter processed the laptop, FBI Special Agent Michael D. Kelley (“Agent Kelley”) performed a substantive review. (*Id.*) During the course of Agent Kelley’s review, he shared the two potentially illegal images from the computer with Hunter. (*Id.*)

In light of the Government’s proffer, this Court stated that “though it’s not part of this record, I think it’s fair to say that there was a consent to search granted by Mr. Nayyar’s wife.” (Tr. 232.) In addition, this Court held that “this issue has been waived.” (Tr. 233.) Alternatively, this Court concluded that “even if that waiver is determined not to be appropriate for some reason, I do think the doctrine of inevitable discovery protects the testimony of Agent Hunter, and I am not going to strike the testimony.” (*Id.*) Accordingly, this Court denied Nayyar’s mistrial motion.

After a seven-day trial, the jury found Nayyar guilty on all counts. (Tr. 737-38.) The evidence obtained illegally from Nayyar’s laptop was a key component of the Government’s case and the resulting convictions.

On October 30, 2014, this Court sentenced Nayyar to an aggregate term of 15 years of imprisonment, as follows: 5 years on each of Counts 1 and 2, to run concurrently; 10 years on each of Counts 3 and 4, to run concurrently to each other and consecutively to Counts 1 and 2; and 5 years on Count 5, to run concurrently to all other counts. Judgment was entered on October 31, 2014.

II. NAYYAR’S APPEAL AND THE SECOND CIRCUIT’S SUMMARY ORDER

Nayyar appealed his conviction to the United States Court of Appeals for the Second Circuit. He argued that this Court erred when it denied his mistrial motion because: (1) he did

not waive his Fourth Amendment claim; (2) there was no valid consent from his wife to search the laptop; (3) the FBI conducted unlawful searches of his laptop before obtaining a warrant; and (4) the evidence was not admissible pursuant to any exception to the exclusionary rule.³

On October 14, 2015, the Court of Appeals issued a summary order (the “Summary Order”), holding that “the district court could not properly deny the suppression motion on this record,” and remanding to this Court “to conduct a post-trial hearing on the issues relating to the computer evidence received at trial.” (Summary Order at 4.) Specifically, the Court of Appeals directed this Court to conduct a hearing on whether “(1) Nayyar waived his right to challenge the evidence in question, (2) Nayyar’s wife’s consent was valid, and (3) the independent source doctrine applies.” (*Id.* at 7.) The Court of Appeals further noted that it would retain jurisdiction over any appeal. (*Id.*)

III. THE STIPULATION

Following the Second Circuit’s decision, the Government conducted further inquiry into the facts surrounding the computer search, and shared those facts with the defense. On June 6, 2016, Mr. Nayyar and the Government reached a stipulation regarding certain facts.⁴ The stipulated facts provide far more detail than—and reveal inaccuracies in—the Government’s mid-trial proffer to the Court. In light of the stipulation, the parties and the Court agreed that the Court need not conduct an evidentiary hearing to resolve the legal questions identified by the Court of Appeals.

³ Nayyar also argued that there was insufficient evidence to support the jury’s verdict on Count 5.

⁴ A copy of the stipulation is being filed concurrently with this memorandum of law.

ARGUMENT

**THE EVIDENCE OBTAINED
FROM MR. NAYYAR'S LAPTOP SHOULD HAVE BEEN SUPPRESSED**

Pursuant to the Summary Order, there are three issues to be addressed by this Court:

- (1) Was the consent of Nayyar's wife valid?
- (2) Does the independent source doctrine apply to these facts?
- (3) Did Nayyar waive his right to challenge the laptop evidence?

Initially, in the middle of trial, this Court addressed the laptop issue on the basis of limited information, primarily the Government's proffer. Now, with the benefit of the extensive supplemental facts agreed upon by the parties, Nayyar submits that this Court should answer each of the questions posed by the Second Circuit in the negative.

I. THE CONSENT OF NAYYAR'S WIFE WAS INVALID

A. Pertinent Facts

1. Nayyar's Wife's Consent to Search

On September 24, 2009, FBI agents, including Agent Kelley, arrested Nayyar at his home pursuant to an arrest warrant. (¶¶ 1-2.)⁵ At the time of the arrest, his then-wife, Maryna Nosava, consented to a search of their residence and executed a written consent form. (¶ 4; Ex. A.)

In the course of their search of the residence, FBI agents identified two laptops. (¶ 7.) Ms. Nosava executed a written consent form for the search of the two laptops. (¶ 8; Ex. B.) Nosava told the FBI agents that she typically used one of the laptops, while Nayyar used the other. (¶ 8.) Based on this information, the agents decided to seize only one of the two laptops—the one used by Nayyar. (¶ 9.)

⁵ Citations to the parties' stipulation dated June 6, 2016 are denominated "¶ ____." Citations to exhibits to the stipulation are denominated "Ex. ____."

In connection with executing the consent form, Nosava told the agents that Nayyar's laptop, unlike hers, was protected by a password. (§ 8.) She provided the agents with the password that she knew for Nayyar's laptop, and the agents recorded that password on the consent form. (*Id.*) In fact, Nosava did *not* know the current password to Nayyar's laptop, because Nayyar had deliberately changed the password without informing her of the current one. (§ 25a.) Approximately one month earlier, Nayyar and Nosava had argued about Nayyar's laptop. (*Id.*) As a result, Nayyar changed the password and did not tell her the new password. (§§ 8, 25a.) Nosava had not used the computer since Nayyar changed the password in or about August 2009. (§ 25a.)

It was not until months later (no earlier than December 21, 2009) that the Government learned that Nosava did not know the password to Nayyar's laptop. (§ 25.) At that time, when agents asked her, Nosava told them about her fight with Nayyar, and the fact that she did not know the new password to the computer. (§ 25a.) When they obtained her consent on September 24, 2009, however, the agents did not ask Ms. Nosava whether the password she provided was current or when she had last used or had access to the laptop. (§ 8.) Nor did they ask Nayyar about his wife's access to the computer or its password during his lengthy post-arrest interview on the same day. (§ 10.) Contrary to the Government's proffer during trial (Tr. 193), Nayyar did not provide them with the password to the computer.

2. The Initial Searches of the Laptop

On December 2, 2009, Agent Hunter began her forensic examination of the laptop. (§ 14.) To do so, she created a forensic copy, the contents of which were identical to the contents of Nayyar's laptop in all respects (the "Forensic Image"). (§ 16.) As described in Agent Hunter's "Examination Notes," the following activities occurred during Hunter's review of the Forensic Image: "Observed the software registry file with AccessData Registry Viewer.

Observed the operating system Windows XP, Service Pack 3 Observed the current time zone was set to Eastern Standard Time with daylight savings enabled.” (¶ 16; Ex. E at 1-2.) The software used to conduct these activities did not require entering a password. (¶ 24d.)

The program used by Agent Hunter generated a log which kept track of all activity conducted on the laptop during her forensic review (“FTK Log-1”). (¶ 17; Ex. H.) On December 7, 2009, Hunter closed FTK Log-1 and opened a new FTK Log (“FTK Log-2”), which kept track of all activity on the laptop thereafter. (¶ 20; Ex. I.)

On December 18, 2009, Agent Kelley started his review of the Forensic Image, which also did not require entering a password. (¶¶ 23-24.) His activities are recorded in FTK Log-2. (See Ex. I.) In the course of his review, Kelley conducted searches for “night vision goggles,” “M-16,” and those two terms combined. (¶ 23a-c.) He also created bookmarks entitled “Graphics of Interest,” “Graphics of Interest 2,” and “Graphics of Interest 3,” and added files to those bookmarks. (¶ 23e-j.) Kelley searched the laptop for more than an hour. (¶ 23.) As discussed on pages 13-14, *infra*, Kelley terminated his initial search of the laptop after consulting with AUSA Buckley about some images he had encountered as well as the legal basis for the search. (¶¶ 25b.)

B. Nosava Could Not Consent to the Search of Nayyar’s Laptop Because the Laptop Was Password-Protected and She Did Not Know the Password

It is a “basic constitutional rule” that warrantless searches are “per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions.” *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971) (internal quotation marks omitted). One such exception is when the search is “conducted pursuant to the consent of an authorized person.” *United States v. Snype*, 441 F.3d 119, 130 (2d Cir. 2006).

The burden is on the Government to prove by a preponderance of the evidence that there was valid consent. *Id.* at 131. A third party “may validly consent to the search of an area in which another has a reasonable expectation of privacy” if two prongs are present: “first, the third party had access to the area searched, and, second, either: (a) common authority over the area; or (b) a substantial interest in the area; or (c) permission to gain access.” *United States v. Davis*, 967 F.2d 84, 87 (2d Cir. 1992). The consent given by Nayyar’s wife fails to satisfy either prong.

First, it is clear that Ms. Nosava did not have access to the laptop. Whether a third party has access “depends on the understandings communicated by the titular owner to that person.” *United States v. McGee*, 564 F.3d 136, 140 (2d Cir. 2009). “The presence or absence of locks . . . can be helpful to the court’s discernment of that understanding.” *Id.* When the titular owner has locked a third party out of a room or container, the third party does not have access. *Id.* A password on a computer or computer file is considered the functional equivalent of a lock. *See Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (noting that “password-protected files are analogous to [a] locked footlocker” and that “[b]y using a password, [defendant] affirmatively intended to exclude” others from accessing the files).

It is undisputed that at the time Nosava purportedly consented to the search of Nayyar’s laptop, the laptop was password-protected and Nosava did not know the password. Indeed, as Nosava knew, Nayyar had deliberately changed the password approximately one month earlier, and had deprived Nosava of any access. (¶25.) Although Nosava could see and touch the laptop that was present in her home, she had no ability to access its contents because she did not know the password. (*Id.*) Accordingly, under the applicable law as set forth above, Nosava did not have access to the laptop. This point is dispositive: the first prong of the *Davis* test is not met, and therefore, Nosava’s consent is invalid.

In any event, the second prong fares no better. “Authority to consent to a search rests on mutual use of the property by persons generally having joint access or control for most purposes” *McGee*, 564 F.3d at 139 (internal quotation marks omitted). When determining whether a third party exercises common authority over the contents of a computer, courts place great weight on “whether password protection is used,” *United States v. Stabile*, 633 F.3d 219, 232 (3d Cir. 2011), and have consistently held that a third party does not have actual authority over password-protected computers or computer files. *See, e.g., United States v. Buckner*, 473 F.3d 551, 554 (4th Cir. 2007) (third party “did not have actual authority to consent to a search of her husband’s password-protected [computer] files”); *Trulock*, 275 F.3d at 403 (same); *United States v. Griswold*, 2011 U.S. Dist. LEXIS 153943, at *11 (W.D.N.Y. June 2, 2011) (defendant’s mother did not have authority to consent to search of his laptop because “the laptop itself is akin to a closed container that has been ‘locked’ by the defendant’s deliberate use of a password”). Nosava did not have common authority over the laptop because Nayyar “locked” it with the new password, and he did not share the new password with Nosava. (¶ 25.)

Nor are the other criteria delineated in the second *Davis* prong satisfied. In light of the password change, it is apparent that Nayyar’s wife did not have “permission to gain access” to the laptop. Finally, Nayyar’s wife did not have a “substantial interest” in the laptop. She told the agents that she used the other laptop, and that this laptop was used by Nayyar. (¶ 8.) Her lack of use of the laptop (and lack of any access for approximately one month prior) make clear that she did not have a substantial interest in it.

Under the *Davis* test, the consent given by Nayyar’s wife is invalid. This invalid consent cannot be salvaged by the doctrine of apparent authority. Apparent authority to give consent is judged against an objective standard: “[W]ould the facts available to the officer at the moment

. . . warrant a man of reasonable caution in the belief that the consenting party had authority over the premises?”” *Illinois v. Rodriguez*, 497 U.S. 177, 188 (1990) (internal quotation marks omitted). Courts routinely hold that no apparent authority exists where the third party explains that an object or container does not belong to her and the officers do not inquire further into the third party’s relationship with the object or container. *See, e.g., United States v. Turner*, 23 F. Supp. 3d 290, 312-13 (S.D.N.Y. 2014); *Griswold*, 2011 U.S. Dist. LEXIS 153943, at *15 (mother did not have apparent authority over son’s laptop where she identified laptop as belonging to her son and distinguished it from the computer she used, and investigators “made absolutely no inquiry about what relationship [the mother] had to the contents of her son’s laptop and instead simply asked her to sign a consent to search form”).

For example, in *United States v. Turner*, the court held that the defendant’s girlfriend did not have apparent authority over the contents of the defendant’s backpack where she identified the backpack and its contents as belonging to the defendant, and “[s]he was not asked any further questions to establish her own ownership, control, or use of the backpack.” 23 F. Supp. 3d at 311. The court emphasized that “the officers were aware of several facts establishing [the defendant’s] ownership and exclusive use of the backpack,” and yet they “decided not to ask—or were negligent in failing to ask—whether [his girlfriend] ever used or accessed” the backpack, its contents, or the surrounding area. *Id.* at 312-13. The court found that “if there was any ambiguity regarding [his girlfriend’s] authority to grant consent to search the bag—and the Court finds that there was not—it was up to the government to dispel it. . . . [T]he police are not free to simply take information at face value.” *Id.* at 312.

Similarly, the agents who seized Nayyar’s laptop were aware of numerous facts establishing Nayyar’s ownership and exclusive use of the laptop: Nosava explicitly told them it

belonged to Nayyar, and distinguished it from the other laptop in their residence which she typically used. (¶ 8.) She also told the agents that Nayyar’s laptop was password-protected. (*Id.*) These facts, like those in *Turner*, “could not have resulted in any uncertainty as to whom the [laptop] belonged.” *Turner*, 23 F. Supp. 3d at 317.

Indeed, the facts here are even starker than in *Turner*. The agents knew that the laptop belonged to Nayyar, not Nosava. They also knew that unlike Nosava’s computer, Nayyar’s laptop was locked. Yet, the agents made no effort whatsoever to determine Nosava’s level of access; they did not ask her whether the password she provided was current or when she had last used the laptop.⁶ (¶ 8.) Nor did they ask Nayyar about Nosava’s relationship to the laptop (or for his consent to search it), although they had every opportunity to do so. (¶ 10.) As in *Turner*, further inquiry by the agents was plainly required. *See Turner*, 23 F. Supp. 3d at 311-13. In these circumstances, a reasonable officer could not have relied on Nosava’s consent, and thus there was no apparent authority. “To hold otherwise would jeopardize the consent doctrine’s intended function as a ‘jealously and carefully drawn exception.’” *Id.* at 311.

C. The Initial Searches Were Unlawful In Light of Nosava’s Invalid Consent

Given that Nosava did not provide valid consent, the FBI’s initial searches of the laptop in December 2009 were unlawful. First, Hunter searched the laptop upon receiving it at the CART unit. Although Hunter’s forensic processing did not entail substantive review (¶ 18), it nonetheless involved going through the laptop’s contents without entering a password. As Hunter’s “Examination Log” noted, she conducted the following activities on the laptop: “Observed the software registry file with AccessData Registry Viewer. Observed the operating system Windows XP, Service Pack 3 Observed the current time zone was set to Eastern

⁶ If they had asked, they would have quickly determined that she did not have authority to consent to the search of the laptop.

Standard Time with daylight savings enabled.” (§ 16; Ex. E at 1-2.) This review process certainly constituted a search, especially given that it involved overstepping Nayyar’s personal password. *See United States v. Syphers*, 426 F.3d 461, 468 (1st Cir. 2005) (referring to forensic review of computer as a “search”); *United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1076 (D.N.D. 2008) (same).

Second, there is no dispute that after Hunter’s initial review, Kelley began a detailed, manual review of the laptop’s contents. This review involved conducting searches for “night vision goggles,” “M-16,” and those two terms combined. (§ 23a-c.) The search for “M-16” returned 34 hits in 16 files, all of which Kelley reviewed. (§ 23d.) Kelley also created bookmarks entitled “Graphics of Interest,” “Graphics of Interest 2,” and “Graphics of Interest 3,” and added files to those bookmarks. (§ 23e-j.) There can be no doubt that this review constituted a warrantless search of Nayyar’s laptop. Absent valid consent, this search was unlawful.

II. THE INDEPENDENT SOURCE DOCTRINE DOES NOT APPLY

A. Pertinent Facts

During his initial search of Nayyar’s laptop on December 18, 2009, Agent Kelley came across two images he believed to be child pornography. (§ 23k.) In view of the images he found, he halted his search of the laptop and contacted AUSA Buckley for guidance. (§§ 23-24.)

On or about December 21, 2009, Agent Kelley informed AUSA Buckley that he had started reviewing the Forensic Image and had identified suspected child pornography. (§ 24.) In light of the potential contraband on the laptop, AUSA Buckley inquired regarding the legal basis for the search. (§ 24b.) Agent Kelley explained that they were relying upon the consent form executed by Nosava. (*Id.*) To ascertain whether that third-party consent was sufficient, AUSA Buckley inquired further, and asked whether the laptop was protected by a password. (§ 24d.)

Agent Kelley responded that the agents had not needed a password in order to conduct their search. (*Id.*) He also noted that the consent form listed a password, but he did not know whether it was valid because the search process had bypassed the laptop's password-protection. (¶ 24e.) AUSA Buckley instructed Agent Kelley to get more information regarding whether Nosava had access to the laptop and knowledge of its password. (¶ 24f.)

In accordance with these instructions, Agent Kelley contacted Nosava. (¶ 25.) He determined that she did not know the password to the computer on the day she executed the consent form, and had not used the computer for approximately one month prior to that date. (*Id.*) Agent Kelley subsequently informed AUSA Buckley that Nosava did not know the current password to the laptop when she consented to the search. (¶ 25a.) Upon learning this information, AUSA Buckley expressed concerns about Nosava's ability to consent to a search of the laptop, and instructed Agent Kelley to halt any further review of the Forensic Image until a search warrant had been obtained. (¶ 25b.)

The Government obtained a search warrant on October 29, 2010, almost a year after the initial searches were conducted by Hunter and Kelley. (*Id.*) After the Government obtained the search warrant, on December 9 and 10, 2010, an individual from the FBI accessed the Forensic Image. (¶ 39; Ex. I.) Almost immediately upon accessing the Forensic Image (and before running searches related to the charges in this case), that individual searched the laptop for child pornography.⁷ (¶ 39; Ex. I at 5.) None was found. (*Id.*)

⁷ On December 9, 2010, the individual ran searches for "727139.jpg," "young asian teenager," "207.226.170.169/animal/727139," and the latter two phrases combined. (¶ 39; Ex. I at 4-5.) These searches each returned hits. (*Id.*) The next day, the individual created a bookmark entitled "possible CP" and added files to that bookmark. (¶ 39g; Ex. I at 4-5.)

B. The Independent Source Doctrine Does Not Apply Because the Government's Search Warrant Application Was Prompted By the Prior, Unlawful Review

The evidence taken from Nayyar's laptop cannot be saved by the "independent source" exception to the exclusionary rule. Under this doctrine, "second-look" warrants may be permitted where the "later, lawful seizure is genuinely independent of an earlier tainted one." *Murray v. United States*, 487 U.S. 533, 542 (1988). The Government bears the burden of establishing by a preponderance of the evidence that the independent source doctrine applies. *Id.* The Government must prove two elements: "(1) the warrant must be supported by probable cause derived from sources independent of the illegal entry; and (2) the decision to seek the warrant may not be prompted by information gleaned from the illegal conduct." *United States v. Johnson*, 994 F.2d 980, 987 (2d Cir. 1993).

With respect to the second element of the *Johnson* test, the court "must consider whether the agents would have applied for a warrant had they not [conducted the illegal search] beforehand." *Id.* See also *Murray*, 487 U.S. at 542 (explaining that the independent source doctrine does not apply where "the agents' decision to seek the warrant was prompted by what they had seen during the initial entry"). In *Johnson*, this second element was established because the decision to seek a warrant was "prompted not by the prior review," but rather by "the district court's indication that a warrant was necessary." 994 F.2d at 987.

Here, the Government's decision to seek a warrant was prompted by the prior review by Agent Kelley. It is undisputed that Agent Kelley halted his search upon encountering images he thought might be child pornography, and contacted AUSA Buckley for guidance. (¶¶ 23-24.) Had he not seen the potential child pornography, Agent Kelley's search would have continued unabated; it was the discovery of possible child pornography during the search that animated the decision to obtain a warrant. This is precisely what the second prong of the *Johnson* test

prohibits. Accordingly, the Government cannot satisfy its burden under the independent source doctrine; the second prong of the *Johnson* test is not and cannot be met.⁸

Moreover, the relationship between Agent Kelley's pre-warrant discovery and the decision to obtain a search warrant is underscored by the Government's actions following the search warrant. When the Government resumed the process of searching the laptop after the search warrant had been obtained, the initial focus was on child pornography. Indeed, the first searches that were run on the laptop after the warrant was obtained were for "727139.jpg," "young asian teenager," "207.226.170.169/animal/727139," and the latter two phrases combined. (¶ 39; Ex. I at 5.) The individual running these searches also created a bookmark entitled "possible CP" and added files to that bookmark. (¶ 39g; Ex. I at 5.) In other words, the Government did not obtain a warrant merely so that it could return to the areas of initial interest; the focus of the computer search had changed in light of Kelley's discovery of the two potentially illegal images. This post-warrant conduct is further evidence that the images Kelley found during the initial, unlawful search were exactly what spurred the Government to pursue a search warrant.⁹

In sum, the Government cannot meet the second element of the *Johnson* test. Thus, the independent source doctrine cannot save the unlawful pre-warrant search, and none of the evidence from Nayyar's laptop should have been admitted at trial. *Cf. United States v. Siciliano*, 578 F.3d 61, 72 (1st Cir. 2009) ("[T]he November 16 search was not an independent source of the evidence discovered in the apartment and subsequently on the seized computers. The evidence was therefore rightly suppressed." (citation omitted)); *United States v. Ortega*, 2007

⁸ The first prong of the *Johnson* test—that the search warrant be supported by probable cause derived from sources independent of the unlawful search—is satisfied. Indeed, the Government omitted any mention of its initial unlawful search or the potential child pornography that it had discovered from the search warrant application.

⁹ The affidavit in support of the search warrant did not reference child pornography, and the warrant did not authorize a search of the laptop for child pornography. (See Ex. G.)

U.S. Dist. LEXIS 82514, *15 (M.D. Fla. Nov. 6, 2007) (“Since the decision to obtain [the] search warrant is tainted . . . [a]ll evidence obtained pursuant to the search warrant must be suppressed.”).

III. NAYYAR DID NOT WAIVE HIS RIGHT TO CHALLENGE THE LAPTOP EVIDENCE

A. The Timing of Discovery and Pretrial Motions to Suppress

On September 1, 2010, included with other discovery, the Government provided the defense with a copy of the written consent form for the laptop signed by Nosava. (¶ 8; Ex. B.) Then, at a conference with this Court on September 16, 2010, the Government indicated that it was planning to obtain a search warrant for Nayyar’s laptop. (¶ 29.) On October 12, 2010, during another conference before this Court, the Government mistakenly asserted that it had already obtained a search warrant. (¶ 30.) The Government also indicated that it did not have the results of any search of the computer available to disclose to the defense, and thus, to the extent the defense sought to suppress any information obtained from a search of the computer, the Government would not object if Nayyar did so after receiving the results of the search. (*Id.*) The Government actually obtained the search warrant on October 29, 2010 (¶ 33), and provided it to the defense on November 8, 2010 (¶ 34).¹⁰

In January 2011, the Government provided the defense with the opportunity to review a “staging media copy” of the Forensic Image (¶¶ 41-42), and a DVD of all images that were recovered from the laptop (¶ 46). On March 22, 2011, the Government also provided a copy of the “FTK Report” created by Agent Hunter. (¶ 23 n.3; Gov’t Ex. 20.) The FTK Report sets forth the steps that the FBI performed on the Forensic Image, although it does not show the dates or times when these activities occurred. (*See* Gov’t Ex. 20.) Indeed, none of the documents

¹⁰ The defense filed a motion to suppress with respect to Nayyar’s post-arrest statements on November 24, 2010. (*See* Docket No. 16.) No motion to suppress the computer evidence was due on this date in light of the Government’s statements on October 12, 2010.

provided to the defense during discovery showed that the FBI had conducted searches on the laptop without entering a password prior to obtaining the search warrant. Accordingly, prior to his trial, Nayyar had no reason to believe that the Government had searched the laptop before obtaining a warrant.

On the eve of Nayyar's trial, the Government produced additional documents relating to the laptop pursuant to its disclosure obligations under the Jencks Act, 18 U.S.C. § 3500. Specifically, on March 14, 2012, among other materials pursuant to § 3500, the Government provided a copy of Agent Hunter's "Communications Log," which contains dated entries of all communications Agent Hunter had in connection with her examination of Nayyar's laptop (¶ 13; Ex. D); and a copy of Agent Hunter's "Examination Notes," which contains the notes written by Agent Hunter regarding steps she took during her examination of the laptop (¶ 14; Ex. E).

Jury selection began on March 15, 2012. At Nayyar's trial, Agent Hunter testified at length about what the FBI found on Nayyar's laptop. During her testimony, the Government introduced as an exhibit the FTK Report in its entirety. (*See* ¶ 23 n.3; Gov't Ex. 20.) The FTK Report shows the bookmarks Kelley created during his search in December 2009 (i.e., "Graphics of Interest 1," "Graphics of Interest 2," and "Graphics of Interest 3"). (*See* Gov't Ex. 20.)

On cross examination, Hunter explained that she had "commenced [her] search" of the laptop on December 2, 2009, although a search warrant was not obtained until October 29, 2010. (Tr. 104-05.) She also testified that Nayyar's laptop was protected by a password, and that she accessed the laptop in December 2009 without knowing the password. (Tr. 102-03.) At this point, Nayyar and his counsel learned for the first time that the FBI had searched Nayyar's personal laptop without a warrant or valid consent. Based on this information, Nayyar moved for a mistrial. (Tr. 190-91.)

Notably, FTK Log-1 and FTK Log-2 were not provided to the defense until May 5, 2016, in connection with the remand proceedings. (¶¶ 17, 20.) In contrast to the FTK Report, these documents do show the dates and times when specific activities were performed by the FBI. (See Exs. H & I.)

B. Nayyar Had Good Cause For Not Challenging the Computer Search Prior to Trial

During trial and on appeal, the Government argued that Nayyar waived his right to challenge the validity of his wife's consent to search the laptop by failing to raise it until trial. To the contrary, Nayyar did not waive his Fourth Amendment claim because he raised it at his very first opportunity to do so. Under Federal Rule of Criminal Procedure 12(c)(3), "[i]f a party does not meet the deadline for making a Rule 12(b)(3) motion, the motion is untimely. But a court may consider the defense, objection, or request if the party shows good cause." Fed. R. Crim. P. 12(c)(3).¹¹

A defendant shows good cause by demonstrating cause for the delay and prejudice. *See Davis v. United States*, 411 U.S. 233, 242 (1973). *See also United States v. Wilson*, 11 F.3d 346, 353 (2d Cir. 1993) (defendant shows good cause by presenting "reasonable excuse" for his delay). "[I]t is clear that where the grounds for the motion are not discoverable by the defendant until after the trial has begun, cause is established." *United States v. Sanchez*, 813 F. Supp. 241, 249 (S.D.N.Y. 1993). *See, e.g., United States v. Scott*, 607 F. App'x 191, 200 (3d Cir. 2015) ("As [defendant] did not have the sealing orders in his possession before trial, the basis for the motion was not 'reasonably available' to him, and we find good cause for [] not making a pre-trial motion to suppress."); *United States v. Jones*, 766 F.2d 994, 999 (6th Cir. 1985) (defendants

¹¹ Although the parties presented this issue on appeal as one of "waiver," the Court of Appeals pointed out that Federal Rule of Criminal Procedure 12 was revised in 2014 to remove the reference to "waiver," although the "applicable standard . . . is unchanged." Summary Order at 5 n.2.

showed good cause where they were “unaware of the grounds for this motion until [a government agent] was called as a witness at trial”); *Sanchez*, 813 F. Supp. at 250 (defendant excused from waiver where “[i]t was only after [government witnesses] testified at trial and described the entire circumstances of how they obtained entry to the apartment” that defendant became aware of basis for his suppression motion).

Nayyar had good cause for not challenging the search prior to trial, because it was not until Agent Hunter’s testimony that the defense became aware of the basis for a motion to suppress. Prior to the trial, the Government included the written consent form in the discovery materials, but specifically indicated at a court conference that it intended to obtain a search warrant and *then* search the computer and provide results to the defense. (¶¶ 29-30.)

After the Government obtained the search warrant, it provided a copy of the warrant and its supporting application to the defense. (¶¶ 8, 34.) Nothing in the warrant application revealed that the Government had conducted any search prior to getting the warrant, and there was no reason for Nayyar or his counsel to think that the Government had done so. (*See Ex. G.*) The other materials regarding the laptop provided by the Government in discovery—namely, the DVD of images and the FTK Report—showed that the FBI had searched Nayyar’s laptop, but did not indicate when those searches occurred.

In light of these materials, Nayyar had no reason to challenge the validity of his wife’s consent prior to trial. If anything, the presence in the discovery of both the consent form and the search warrant demonstrated that the Government was not relying on any purported consent for admission of the laptop evidence, because it had gone to the effort of obtaining a subsequent court-authorized search warrant. Moreover, the fact that the Government indicated it did not have search results to provide to the defense as late as October 12, 2010 gave Nayyar no reason

to believe that any search had already occurred prior to the issuance of the warrant. Since Nayyar was not asserting a challenge to the search warrant itself, he had no basis for pressing a suppression motion.

In addition, given that Nayyar and his counsel believed the Government was relying on the search warrant as its legal authority for the searches, Nayyar had no reason to scour all of the § 3500 material—including Agent Hunter’s “Communications Log” and “Examination Notes”—which was provided to the defense only on the eve of trial (long after the appropriate time for filing suppression motions) for any indication that the Government had conducted an undisclosed, pre-warrant search. In any event, Nayyar would not have learned from these materials precisely what occurred before the warrant was obtained. The only materials showing exactly what occurred and when are the FTK Logs. (*See* Exs. H & I.) It is undisputed that these logs were not provided to the defense before trial.¹²

It was not until Agent Hunter testified at Nayyar’s trial that it became clear that the FBI had conducted searches of the laptop without entering the password and prior to getting the warrant. At that point, after the evidence from Nayyar’s laptop had already been admitted, the consent of Nayyar’s wife became relevant for the first time. As soon as these facts became clear, Nayyar moved for a mistrial. (Tr. 190-91.)

Under these circumstances, Nayyar had good cause for not challenging the validity of his wife’s consent prior to trial. *Cf. Scott*, 607 F. App’x at 200; *Jones*, 766 F.2d at 999; *Sanchez*, 813 F. Supp. at 250. In light of the Government’s evident reliance on the search warrant, and not on consent, there was no reason for Nayyar to litigate the consent issue. To hold otherwise would invite—and indeed require—defendants to make unnecessary motions to suppress even in

¹² Indeed, these logs were not provided until after Nayyar’s appeal, in connection with proceedings on remand. (¶¶ 17-20.)

the face of a valid basis for admitting evidence (such as a search warrant) to rule out any other potential basis for admitting that evidence. Imposing that requirement would result in wasteful motion practice and place an undue burden on defendants and district courts. *See Sanchez*, 813 F. Supp. at 250 (“It would hardly be an efficient use of court resources to require defense lawyers to make motions prior to trial without a sufficient basis merely in order to preserve the timeliness of such motions.”).

Furthermore, Nayyar was clearly prejudiced by the improper admission of the laptop evidence. *Cf. United States v. Gonzalez*, 81 F. Supp. 3d 1212, 1225 (D.N.M. 2015) (describing prejudice as “the importance of the motion to the defendant’s case and constitutional rights”). On the first and second days of trial, Agent Hunter testified at length about what the FBI found on Nayyar’s laptop, and the Government introduced numerous exhibits showing that an individual using Nayyar’s account visited websites relating to weapons and military equipment, including guns and night vision goggles. (*See* Tr. 72-75.) One of those exhibits—Government Exhibit 20, the FTK Report—contained bookmarks created by Kelley in his initial unlawful search in 2009. (*See* ¶ 23 n.3; Gov’t Ex. 20.) This evidence was crucial to the Government’s case against Nayyar, particularly with respect to Count 4 (*see* Tr. 696 (noting that the Government had to prove that Nayyar “attempted to provide guns, ammunition, vehicles, bulletproof vests, night vision goggles to Hizballah,” and that he “knew that providing the materials to Hizballah was unlawful”)), and Count 5 (*see* Tr. 702 (noting that the Government had to prove that Nayyar conspired to be a dealer in firearms and ammunition)).

During Hunter’s testimony, the Government also introduced and Hunter discussed a news article describing Israel’s view of Hizballah, which an individual using Nayyar’s account visited in August 2009. (Tr. 95-97.) The article noted that Hizballah had been responsible for carrying

out several terrorist attacks in the 1990s. (Tr. 96-97.) This article found on Nayyar's laptop was the only evidence regarding Nayyar's knowledge that Hizballah was a designated terrorist organization at the time of the offense (*see* Tr. 98), which the Government had to show to meet its burden for Count 2 (attempt to provide material support for Hizballah). (Tr. 686.) Indeed, the Government relied on this evidence in its summation to prove Nayyar's knowledge. (Tr. 568.)

In short, the evidence obtained from the laptop should have been suppressed (and not admitted at Nayyar's trial), and the admission of the laptop evidence was prejudicial to Nayyar. *Cf. Gonzalez*, 81 F. Supp. 3d at 1227 (finding that defendant would be prejudiced where evidence that defendant sought to suppress would, if allowed, "certainly make it more difficult for [defendant] to obtain an acquittal").

CONCLUSION

For the foregoing reasons, the consent of Nayyar's wife was invalid, the independent source doctrine does not apply to the laptop search, and Nayyar did not waive his right to challenge the evidence taken from his laptop. Accordingly, the evidence obtained from Nayyar's laptop should have been suppressed and should not have been admitted at his trial.

Dated: June 17, 2016
New York, NY

Respectfully submitted,

COOLEY LLP

By: /s/ Laura Grossfield Birger

Laura Grossfield Birger
Stephanie B. Turner
1114 Avenue of the Americas
New York, NY 10036
(212) 479-6000
*Attorneys for Defendant
Patrick Nayyar*